

NetStalker and HP Open View

615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
		<p>The most efficient means of protecting this connection between the NSC router client and the <i>NetStalker</i> is to use separate BorderGuard routers between the <i>NetStalker</i> platform and the network, and then to configure an encrypted tunnel between the client router and the "guard" router that protects the <i>NetStalker</i> platform. Since all IP traffic between the <i>NetStalker</i> platform and client is encrypted on the network, the encryption provides confidentiality, integrity, and mutual authentication of the communicating parties.</p> <p>Alternatively, the <i>NetStalker</i> platform can be located on an individual network segment that is directly connected to a dedicated port on the router it is monitoring." p. 1-4. [SYM_P_0079562]</p> <p>"Before <i>Netstalker</i> can protect your network, you must configure the program for your site by setting up the routers to be monitored. This chapter describes how to add and edit client routers listed in the <i>NetStalker</i> window. It also describes how to verify the client information . . ." pp. 3-1-3-6. [SYM_P_0079577-SYM_P_0079582]</p>	<p>such as geographic maps and floor plans as backgrounds for your map to provide "real world" visual references for your network." (1-2) [SYM_P_0080958]</p> <p>"The Component symbol set contains various network components such as hubs, routers, and multiplexers. OpenView applications can add symbols or delete symbols from the standard set." (3-14) [SYM_P_0080996]</p> <p>"Implicit in the SNNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements." (RFC 1157 p. 4) [SYM_P_0527111]</p> <p>"Upon receiving a subtree, the enterprise may, for example, define new MIB objects in this subtree. In addition, it is strongly recommended that the enterprise will also register</p>

NetStalker and HP Open View

615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
			<p>its networking subsystems under this subtree, in order to provide an unambiguous identification mechanism for use in management protocols. For example, if the "Flintstones, Inc." enterprise produced networking subsystems, then they could request a node under the enterprises subtree from the Internet Assigned Numbers Authority. Such a node might be numbered:</p> <p>1.3.6.1.4.1.42</p> <p>The "Flintstones, Inc." enterprise might then register their "Fred Router" under the name of:</p> <p>1.3.6.1.4.1.42.1.1" (RFC 1155 p. 6) [SYM_P_0501017]</p> <p>"See also the Host and Gateway Requirements RFCs for more specific information on the applicability of this standard." (RFC 1155 p. 1) [SYM_P_0501013]</p> <p>"sysServices OBJECT-TYPE layer functionality 1 physical (e.g., repeaters) 2 datalink/subnetwork (e.g., bridges) 3 internet (e.g., IP gateways) 4 end-to-end (e.g., IP hosts)</p>

NetStalker and HP Open View

Claim number	Claim Term	NetStalker (public use / on sale)	HP Open View (printed publication and public use)
			<p>7 applications (e.g., mail relays)</p> <p>For systems including OSI protocols, layers 5 and 6 may also be counted.” (RFC 1213 p. 14) [SYM_P_0501155-SYM_P_0501156]</p> <p>“ipForwarding OBJECT-TYPE SYNTAX INTEGER { forwarding(1), -- acting as a gateway not-forwarding(2) -- NOT acting as a gateway }” (RFC 1213 p. 25) [SYM_P_0501165]</p> <p>“Remote network monitoring devices are instruments that exist for the purpose of managing a network. Often these remote probes are stand-alone devices ... An organization may employ many of these devices, one per network segment, to manage its internet.” (RFC 1271 p. 3) [SYM_P_0501208]</p> <p><u>103:</u></p> <p>SunScreen Firewall. See SunScreen EFS Configuration and Management Guide, Release 1.1 (June 1997) [SUN_0000501-856].</p>

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
	detecting, by the network monitors, suspicious network activity based on analysis of the network traffic data;	See '615 claim 1	See '615 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '615 claim 1	See '615 claim 1
45	The method of claim 44, wherein said integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
46	The method of claim 44, wherein said integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
47	The method of claim 44, wherein the plurality of network monitors include an API for encapsulation of	See '203 claim 4	See '203 claim 4

NetStalker and HP Open View

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
48	monitor functions and integration of third-party tools. The method of claim 44, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.	See '615 claim 1	See '615 claim 1
49	The method of claim 44, wherein said deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7	See '203 claim 7
50	The method of claim 49, wherein said receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors	See '203 claim 8	See '203 claim 8

NetStalker and HP Open View

Claim number	Claim Term	NetStalker (public use / on sale)	HP Open View (printed publication and public use)
51	within the domain monitor's associated network domain. The method of claim 44, wherein said deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
52	The method of claim 51, wherein said receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10	See '203 claim 10
64	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising: deploying a plurality of network monitors in the enterprise network, wherein at	See '615 claim 1	See '615 claim 1
		"NetStalker monitors all events reported from client NSC routers and PCF filters. Based on Haystack Labs' patent pending technology, NetStalker automatically identifies network attacks and attempts to	"To start a discovery, you need to know some information about your own network and the networks you want Autodiscovery to search. To run an IP discovery, you must

NetStalker and HP Open View

Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
615	least one of the network monitors is deployed at a firewall;	<p>exploit TCP/IP protocol vulnerabilities in real using information stored in an internal database, the misuse signature database." p. 1-2. [SYM_P_0079560]</p> <p><i>"Initial PC Filter Configuration"</i></p> <p><i>NetStalker</i> has a standard set of named PCF filters that are used on NSC routers with router sensors to produce the messages used to communicate between the NSC router and <i>NetStalker</i>. The filters are created and downloaded to the router when you run the shell, INSTALL.filters. See Chapter 2 for information on installing <i>NetStalker</i>." p.1-4. [SYM_P_0079562]</p> <p><i>"Securing the Connection"</i></p> <p>Since the <i>Netstalker</i> server platform can be located anywhere on the network, there is the potential of an attacker manipulating the connection between the router and the <i>NetStalker</i> server platform.</p> <p>The most efficient means of protecting this connection between the NSC router client and the <i>NetStalker</i> is to use separate BorderGuard routers between the <i>NetStalker</i> platform and the network, and then to configure an encrypted tunnel between the client router and the "guard" router that protects the <i>NetStalker</i> platform. Since all IP traffic between the <i>NetStalker</i> platform and client is encrypted on the</p>	<p>provide the following information:</p> <p>... The IP address and community name for your default gateway or router if present." (2-2) [SYM_P_0080966]</p> <p>"Devices in the network are displayed on maps. Devices and subnetworks can be organized into submaps to suit your needs. You can create separate submaps of devices grouped by device function, network function, network organization, or corporate organization. You can use the maps to manage your network from a single display even when the network includes devices from different manufacturers. Programs that manage hubs, routers, servers, and other network devices can run in the background. Changes in network status are displayed on network maps with icons representing devices. Color is used to indicate device status. Submaps allow you to create several views of your network to simplify management. You can add meaningful graphics such as geographic maps and floor plans as backgrounds for your map to provide "real world" visual references for your network." (1-2) [SYM_P_0080958]</p> <p>"The Component symbol set contains various network components such as hubs, routers, and multiplexers. OpenView applications can add symbols or delete symbols from the standard set." (3-14) [SYM_P_0080996]</p>

NetStalker and HP Open View

Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
615		<p>network, the encryption provides confidentiality, integrity, and mutual authentication of the communicating parties.</p> <p>Alternatively, the <i>NetStalker</i> platform can be located on an individual network segment that is directly connected to a dedicated port on the router it is monitoring." p.1-4. [SYM_P_0079562]</p> <p>"When you install <i>NetStalker</i> using default values, the entire collection of common filters is installed on the router. Figure 2-2 shows which filters are nested into collections of filters and describes the use of filters.</p>	<p>"Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements." (RFC 1157 p. 4) [SYM_P_0527111]</p> <p>"Upon receiving a subtree, the enterprise may, for example, define new MIB objects in this subtree. In addition, it is strongly recommended that the enterprise will also register its networking subsystems under this subtree, in order to provide an unambiguous identification mechanism for use in management protocols. For example, if the "Flintstones, Inc." enterprise produced networking subsystems, then they could request a node under the enterprises subtree from the Internet Assigned Numbers Authority. Such a node might be numbered:</p>

NetStalker and HP Open View

[illegible]

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
			<p>SYNTAX INTEGER { forwarding(1), -- acting as a gateway not-forwarding(2) -- NOT acting as a gateway }” (RFC 1213 p. 25) [SYM_P_0501165]</p> <p>“Remote network monitoring devices are instruments that exist for the purpose of managing a network. Often these remote probes are stand-alone devices ... An organization may employ many of these devices, one per network segment, to manage its internet.” (RFC 1271 p. 3) [SYM_P_0501208]</p>
	detecting, by the network monitors, suspicious network activity based on analysis of network traffic data;	See '615 claim 1	See '615 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '615 claim 1	See '615 claim 1
65	The method of claim 64, wherein said integrating comprises correlating intrusion	See '203 claim 2	See '203 claim 2

NetStalker and HP OpenView

Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
	reports reflecting underlying commonalities.		
66	The method of claim 64, wherein said integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
67	The method of claim 64, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
68	The method of claim 64, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.	See '615 claim 1	See '615 claim 1
69	The method of claim 64,	See '203 claim 7	See '203 claim 7

NetStalker and HP OpenView

Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
	wherein said deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.		
70	The method of claim 69, wherein said receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8	See '203 claim 8
71	The method of claim 64, wherein said deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
72	The method of claim 71, wherein said receiving and integrating is performed by an enterprise monitor with respect	See '203 claim 10	See '203 claim 10

NetStalker and HP OpenView

'615 Claim number	Claim Term	NetStalker (public use./on sale)	HP OpenView (printed publication and public use)
84	<p>to a plurality of domain monitors within the enterprise network.</p> <p>An enterprise network monitoring system comprising:</p> <p>a plurality of network monitors deployed within an enterprise network, wherein at least one of the network monitors is deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers, firewalls}; said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data;</p>	<p>See '615 claim 1</p> <p>"NetStalker monitors all events reported from client NSC routers and PCF filters. Based on Haystack Labs' patent pending technology, NetStalker automatically identifies network attacks and attempts to exploit TCP/IP protocol vulnerabilities in real using information stored in an internal database, the misuse signature database." p. 1-2. [SYM_P_0079560]</p> <p>"Initial PC Filter Configuration</p> <p>NetStalker has a standard set of named PCF filters that are used on NSC routers with router sensors to produce the messages used to communicate between the NSC router and NetStalker. The filters are created and downloaded to the router when you run the shell, INSTALL.filters. See Chapter 2 for information on installing NetStalker." p. 1-4. [SYM_P_0079562]</p> <p>"Securing the Connection</p> <p>Since the Netstalker server platform can be located anywhere on the network, there is the potential of an attacker manipulating the connection between the router and the NetStalker server platform.</p>	<p>See '615 claim 1</p> <p>"To start a discovery, you need to know some information about your own network and the networks you want Autodiscovery to search. To run an IP discovery, you must provide the following information:</p> <p>...</p> <p>The IP address and community name for your default gateway or router if present." (2-2) [SYM_P_0080966]</p> <p>"Devices in the network are displayed on maps. Devices and subnetworks can be organized into submaps to suit your needs. You can create separate submaps of devices grouped by device function, network function, network organization, or corporate organization. You can use the maps to manage your network from a single display even when the network includes devices from different manufacturers. Programs that manage hubs, routers, servers, and other network devices can run in the background. Changes in network status are displayed on network maps with icons representing devices. Color is used to indicate device status. Submaps allow you to create several views of your network to simplify management. You can add meaningful graphics</p>

NetStalker and HP OpenView

Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
		<p>The most efficient means of protecting this connection between the NSC router client and the <i>NetStalker</i> is to use separate BorderGuard routers between the <i>NetStalker</i> platform and the network, and then to configure an encrypted tunnel between the client router and the "guard" router that protects the <i>NetStalker</i> platform. Since all IP traffic between the <i>NetStalker</i> platform and client is encrypted on the network, the encryption provides confidentiality, integrity, and mutual authentication of the communicating parties.</p> <p>Alternatively, the <i>NetStalker</i> platform can be located on an individual network segment that is directly connected to a dedicated port on the router it is monitoring." p. 1-4. [SYM_P_0079562]</p> <p>"When you install <i>Netstalker</i> using default values, the entire collection of common filters is installed on the router. Figure 2-2 shows which filters are nested into collections of filters and describes the use of filters.</p>	<p>such as geographic maps and floor plans as backgrounds for your map to provide "real world" visual references for your network." (1-2) [SYM_P_0080958]</p> <p>"The Component symbol set contains various network components such as hubs, routers, and multiplexers. OpenView applications can add symbols or delete symbols from the standard set." (3-14) [SYM_P_0080996]</p> <p>"Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements." (RFC 1157 p. 4) [SYM_P_0527111]</p> <p>"Upon receiving a subtree, the enterprise may, for example, define new MIB objects in this subtree. In addition, it is strongly recommended that the enterprise will also register</p>

NetStalker and HP Open View

Claim number	Claim Term	NetStalker (public use / on sale)	HP Open View (printed publication and public use)
			<p>7 applications (e.g., mail relays)</p> <p>For systems including OSI protocols, layers 5 and 6 may also be counted.” (RFC 1213 p.14) [SYM_P_0501155-SYM_P_0501156]</p> <p>“ipForwarding OBJECT-TYPE SYNTAX INTEGER { forwarding(1), -- acting as a gateway not-forwarding(2) -- NOT acting as a gateway }” (RFC 1213 p. 25) [SYM_P_0501165]</p> <p>“Remote network monitoring devices are instruments that exist for the purpose of managing a network. Often these remote probes are stand-alone devices ... An organization may employ many of these devices, one per network segment, to manage its internet.” (RFC 1271 p. 3) [SYM_P_0501208]</p>
	said network monitors generating reports of said suspicious activity; and one or more hierarchical monitors in the enterprise network, the hierarchical	See '615 claim 1	See '615 claim 1
		See '615 claim 1	See '615 claim 1

NetStalker and HP Open View

'615 Claim number	Claim Term	NetStalker (public use / on sale)	HP Open View (printed publication and public use)
	monitors adapted to automatically receive and integrate the reports of suspicious activity.		
85	The system of claim 84, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
86	The system of claim 84, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
87	The system of claim 84, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
88	The system of claim 84, wherein said network traffic data is selected from one or more of the following	See '615 claim 1	See '615 claim 1

NetStalker and HP OpenView

Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
	categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.		
89	The system of claim 84, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7	See '203 claim 7
90	The system of claim 89, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8	See '203 claim 8
91	The system of claim 84, wherein the plurality of network monitors include a	See '203 claim 9	See '203 claim 9

NetStalker and HP OpenView

Claim number	Claim Term	NetStalker (public use / on sale)	HP OpenView (printed publication and public use)
	plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.		
92	The system of claim 91, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10	See '203 claim 10